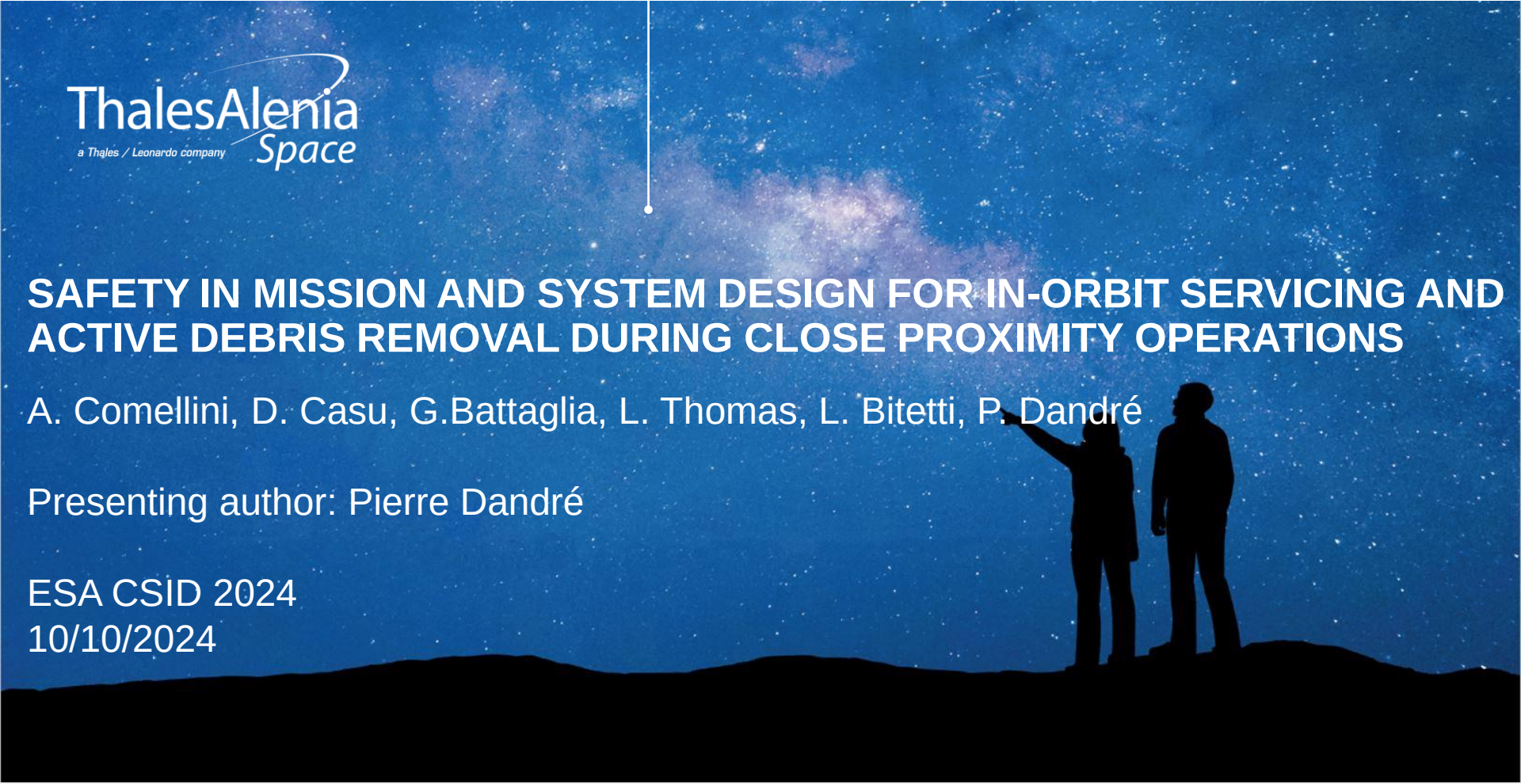
SAFETY IN MISSION AND SYSTEM DESIGN FOR IN-ORBIT SERVICING AND ACTIVE DEBRIS REMOVAL DURING CLOSE PROXIMITY OPERATIONS

A. Comellini, D. Casu, G.Battaglia, L. Thomas, L. Bitetti, P. Dandré

Presenting author: Pierre Dandré

ESA CSID 2024
10/10/2024



Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

/// What does Mission Safety correspond to?

- For uncrewed missions, safety in Close proximity Operations (CPO) translates into avoiding the generation of debris, due to:
  1. Unintentional breakup of the servicer or the client.
  2. Intentional generation of micro-debris during the servicing operations (e.g., caused by the use of some capture method such as harpoons, intentional perforation of S/C surfaces such as MLI to enable refuelling operations, etc …).
  3. Collision of the servicer or the client with third parties.
  4. Unintentional degradation of the client (or the servicer) performance during servicing operations, preventing the client (or the servicer) from continuing its nominal mission after the IOS and precluding the possibility of carrying out End-Of-Life disposal.
  5. Collision of the stack with third parties.
  6. Collision of the servicer with the client.

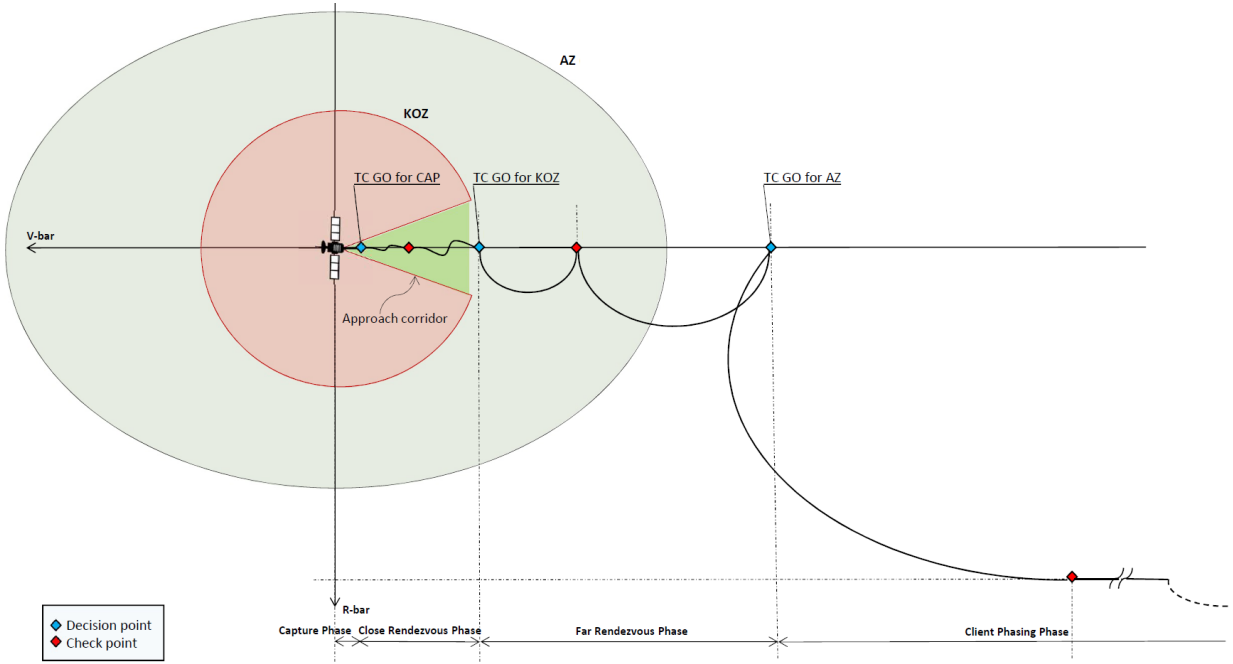
Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TABLE OF CONTENTS

KEY SAFETY REQUIREMENTS

/// Zones and Phases

- Two zones are identified, that can be entered only after positive assessment of a set of conditions (GO/NO-GO)

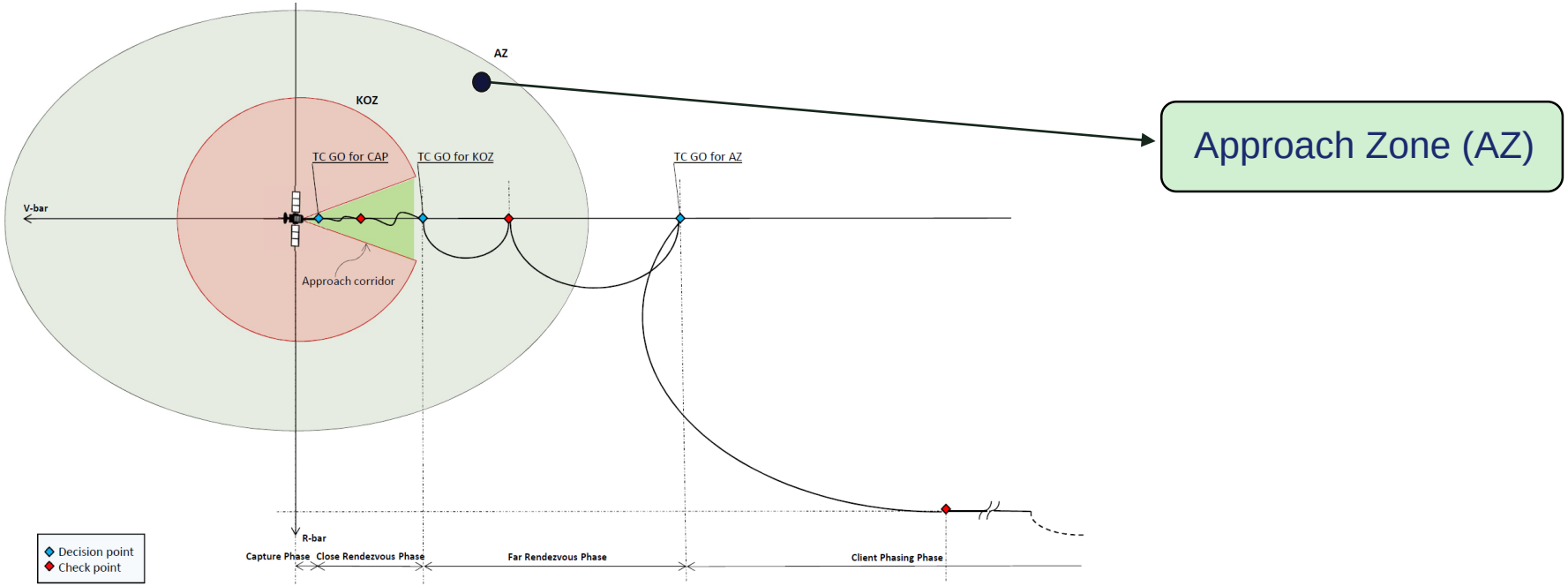


Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

KEY SAFETY REQUIREMENTS

/// Zones and Phases

- Two zones are identified, that can be entered only after positive assessment of a set of conditions (GO/NO-GO)

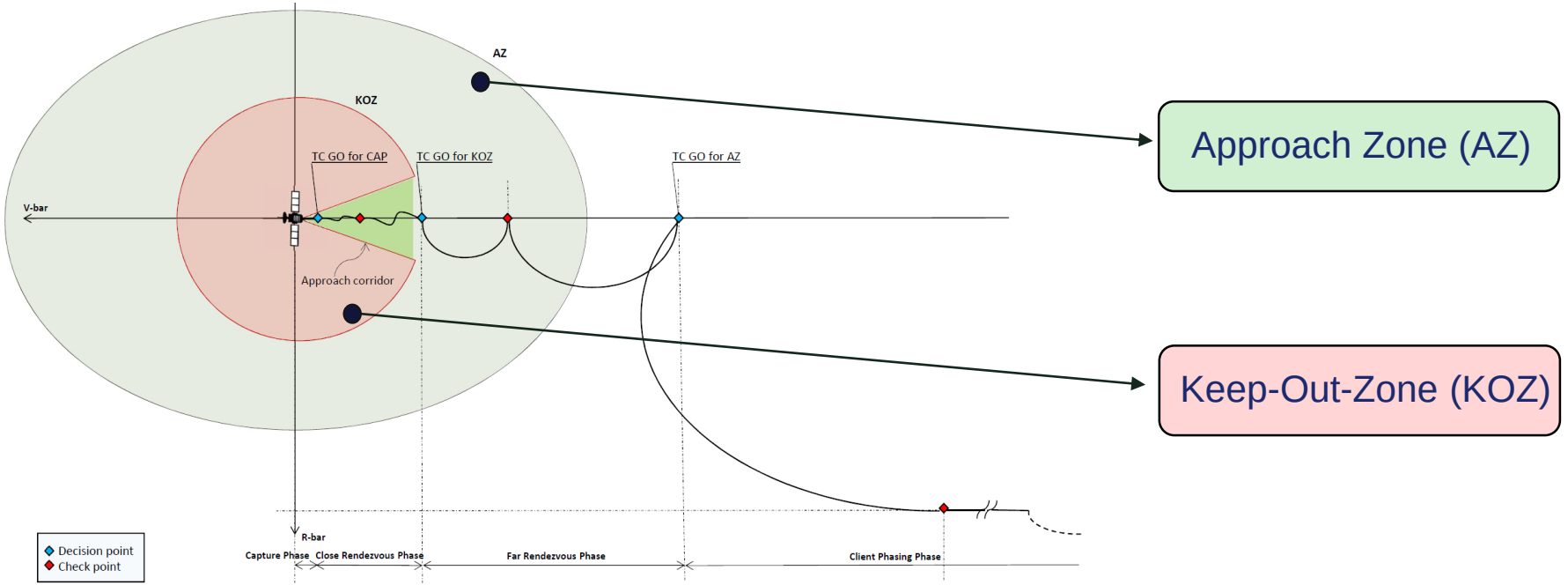


Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

KEY SAFETY REQUIREMENTS

/// Zones and Phases

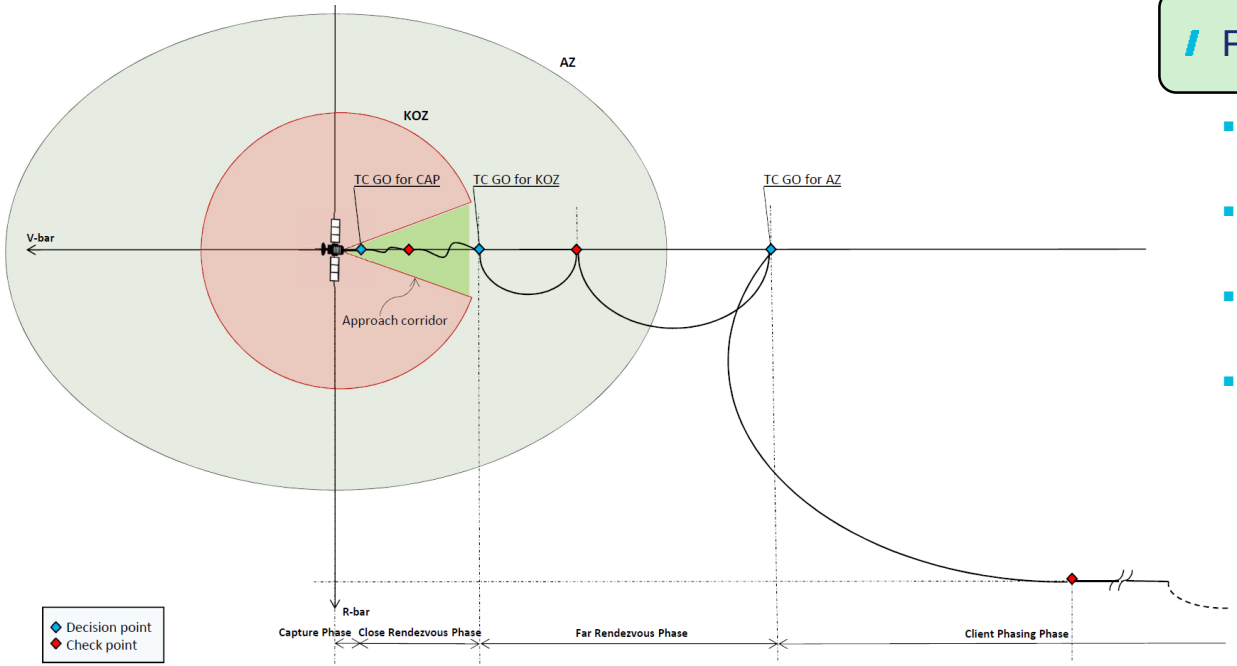
- Two zones are identified, that can be entered only after positive assessment of a set of conditions (GO/NO-GO)



Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

KEY SAFETY REQUIREMENTS

/// Zones and Phases



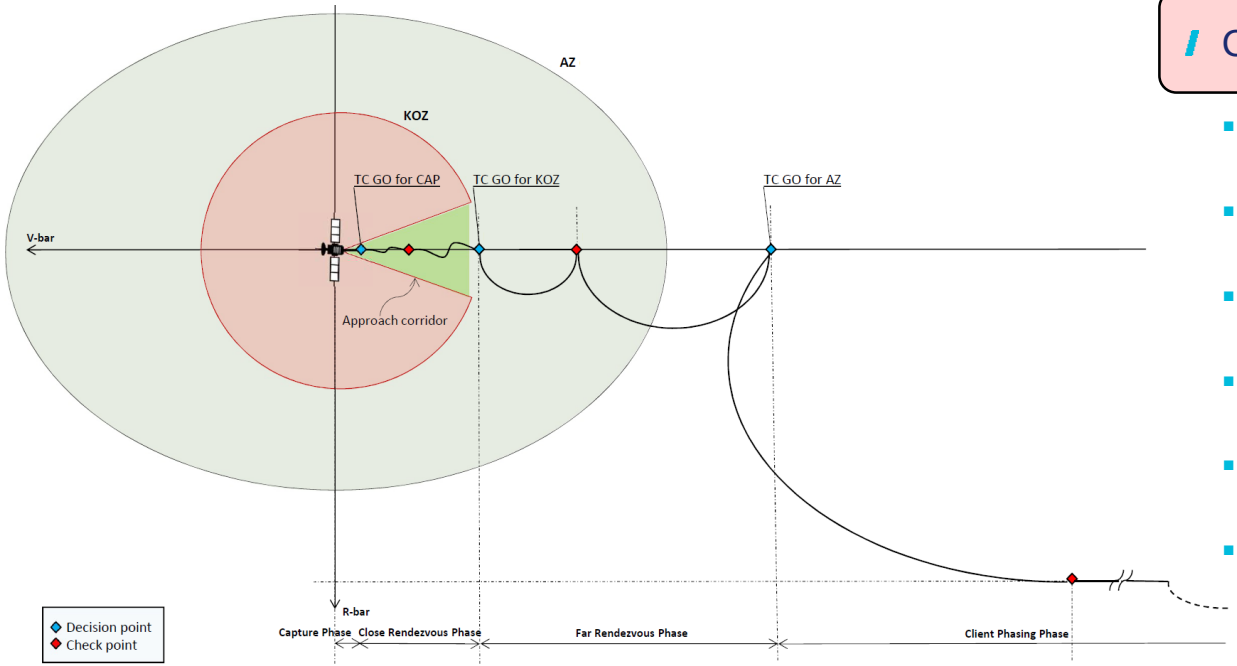
Far Rendezvous Phase:

- Initiated by the GO for Approach Zone
- Any trajectory allowed
- 3-DOF relative estimation
- Autonomous or Ground triggered:
  - Abort (mission safety)
  - Cancel (mission success)

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

KEY SAFETY REQUIREMENTS

/// Zones and Phases



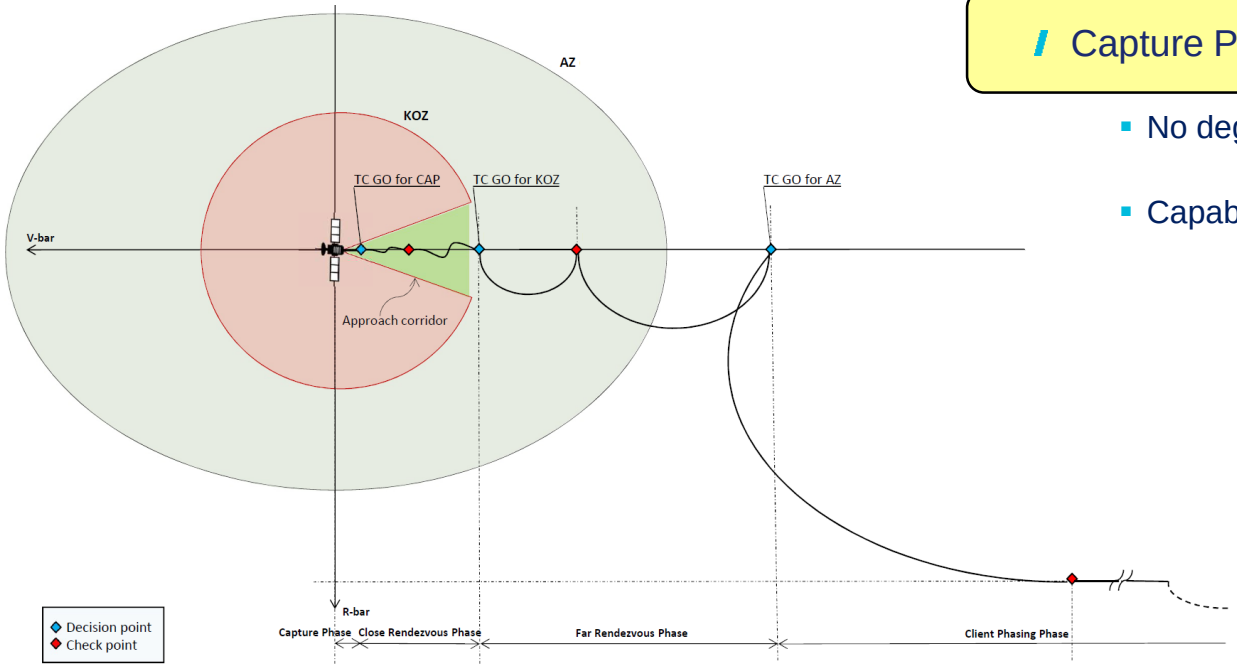
Close Rendezvous Phase:

- Initiated by the GO for Keep-Out-Zone
- Servicer within the Approach Corridor
- Closed loop 6-DOF relative control
- No crossing of clearance envelopes
- Abort Corridor
- Autonomous Abort execution

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

KEY SAFETY REQUIREMENTS

/// Zones and Phases



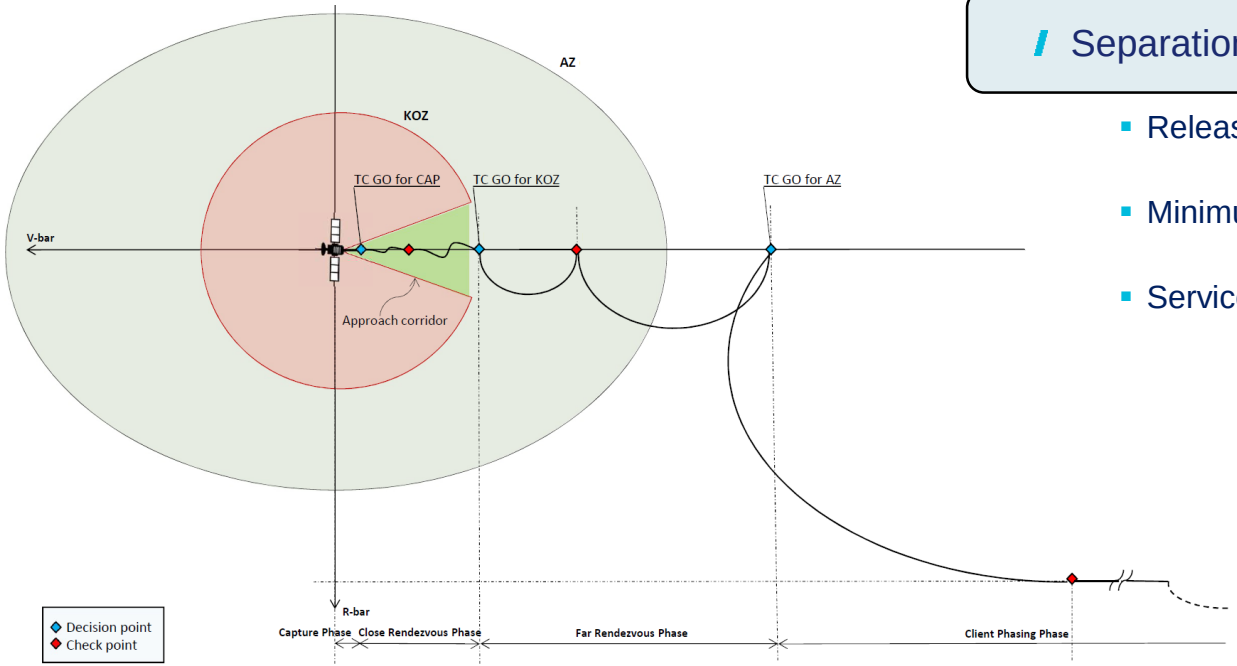
/ Capture Phase, Stack Configuration Phase:

- No degradation of client integrity/performance
- Capability to control the orbit and attitude of the Stack

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

KEY SAFETY REQUIREMENTS

/// Zones and Phases



/ Separation phase, Departure phase:

- Release conditions compatible with control capabilities
- Minimum separation at release before first burn
- Servicer to respect the departure corridor

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TABLE OF CONTENTS

TRAJECTORY DESIGN AND VALIDATION

/// Thales Alenia Space « Rendezvous Trajectory Design & Validation tool » (RTDV)

- **Goal:** fast analysis solution to compare rendezvous strategies through **stochastic analysis**
  - passively safe trajectories validation
  - hold points definition
  - collision avoidance maneuvers strategy validation
  - GNC architectures implementation and performance evaluation
  - Rendezvous sensors and navigation chain performance and trade-off
  - …
- RTDV tool **type of analysis**:
  - Linear Covariance Analysis (LCA) for fast design and prototyping
  - High-scale Monte Carlo campaigns for *V&V purposes* (e.g., robustness, sensitivity and performance campaigns)
- **Scope**:
  - RTDV fills the gap between Mission Analysis and GNC disciplines in the scope of rendezvous missions V&V
  - The tool works alongside the Functional Engineering Simulator (FES) to corroborate the design and verify GNC requirements related to trajectories performance and safety

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TRAJECTORY DESIGN AND VALIDATION

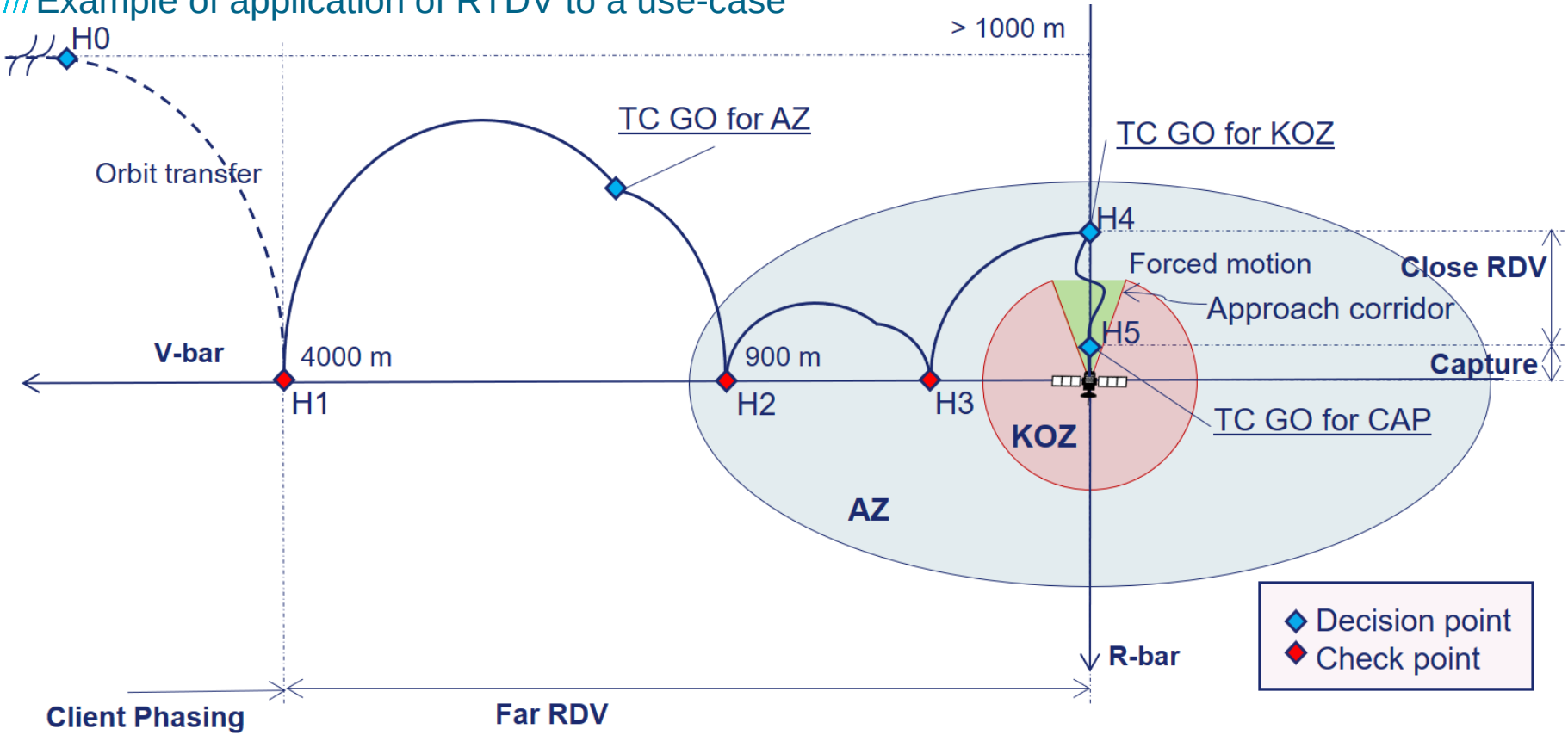
/// Thales Alenia Space « Rendezvous Trajectory Design & Validation tool » (RTDV)

- **Features**:
  - Accurate orbit propagation with complete perturbation model (i.e., drag, solar radiation pressure, gravity potential, third body effect)
  - Attitude dynamic implementation is optional
  - Simplified though representative GNC implementation:
    - The tool directly uses actual OBSW GNC unitary functions (Navigation, Guidance), building blocks of TAS GNC auto-coding framework.
    - Measurement models and state dispersions are correlated with FES setup, sensors models are simplified with respect to FES.
  - Ability to perform stochastic analysis (e.g., LCA, Monte Carlo analysis)
  - Ability to extract overall indexes for the scenario (e.g., probabilities, distributions, parameters values)
    - State estimation error covariance
    - Delta-V covariance
    - Realization error covariance
    - Probability of collision
    - Range and Line-of-Sight estimation error covariance
    - OBSW Guidance and Navigation functions tuning
    - …

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TRAJECTORY DESIGN AND VALIDATION

/// Example of application of RTDV to a use-case



Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TRAJECTORY DESIGN AND VALIDATION

/// Example of application of RTDV to a use-case: Hop1 from H1 to H2

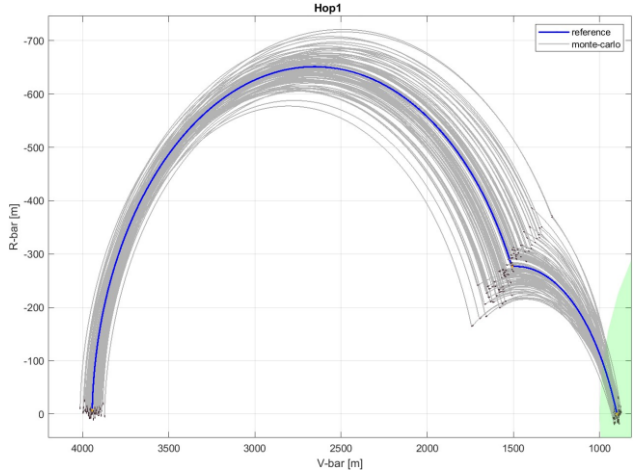


Fig.1

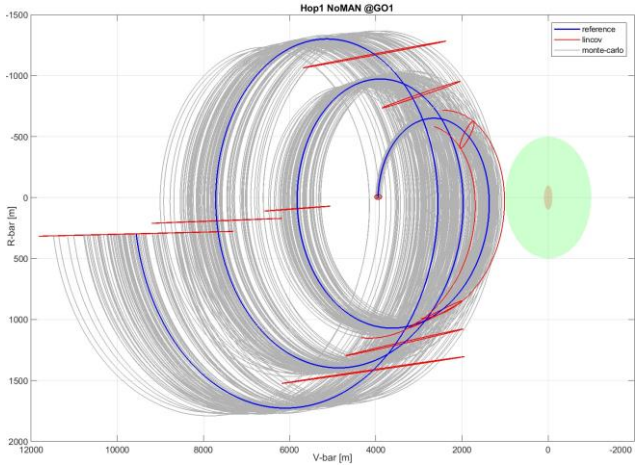


Fig.2

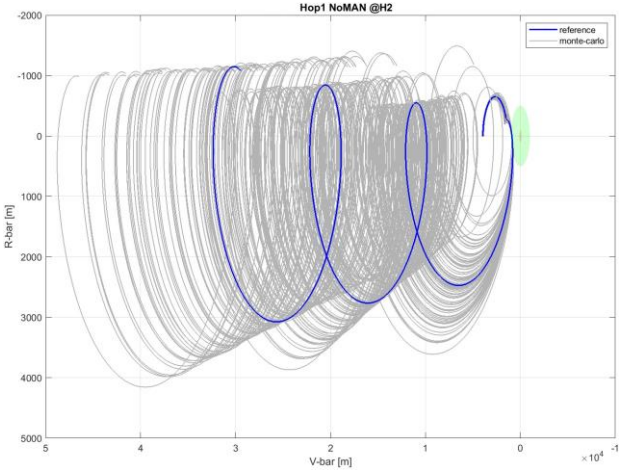


Fig.3

- Nominal scenario (**Fig.1**):
  - servicer successfully (at 3-sigma) enters the AZ after the “GO for AZ” maneuver
- Failure scenario:
  - servicer does not re-enter the AZ in case of no “GO for AZ” (**Fig.2**)
  - failure case after the second maneuver (no braking boost), mostly safe, except for a very little number of limit cases (**Fig.3**)

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TABLE OF CONTENTS

COLLISION RISK ASSESSMENT

/// Requirements

ESA Space Debris Mitigation Requirements – 30/10/2023 - ESSB-ST-U-007 Issue 1 §5.3.3.4

- The probability of unintentional contact between space objects as a result of close proximity operations, or formation flying, in Earth orbit, shall be below **10-4**

ESA GUIDELINES ON SAFE CLOSE PROXIMITY OPERATIONS -12/04/2024 –Issue 3.0

- The servicer ensures that the probability of collision risk with the client (or other rendezvous space object) during the mission is lower than **10-4**
- Note 1: The probability of collision is computed at all times as per orbital plan, especially for critical phases (CR, CAP, SEP,CAM).
- Note 2: Probability of collision is computed for critical phases and in presence of major failures (through in-orbit safety analysis, FDIR concept and autonomy, contingency analysis).

French Space law (LOS) – 2024 - Article 47-16

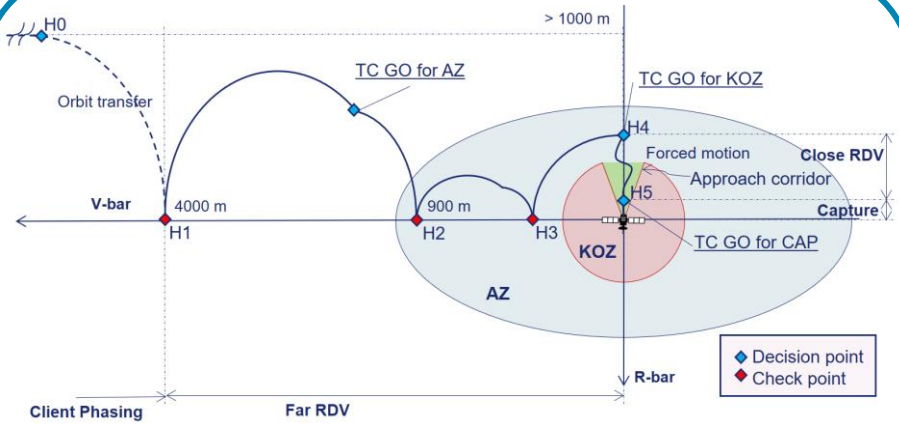
- During the approach phase, the probability to violate flight corridors as defined in the operational concepts of approach and docking and thus to have a collision between the two vehicles shall be below **10-2** per approach and **5E-2** on the overall vehicle lifetime

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

COLLISION RISK ASSESSMENT

/// Methodology proposed:

- The segmentation of the mission **in different phases, as per CONOPS**
- On each phase, a **Fault Tree Analysis (FTA)** conducted taking into account:
  - On the **servicer** side:
    - Hardware failures
    - Single Event Effect
    - Reliability of the Collision Avoidance Manoeuvre (CAM)
    - Common Cause Failures
    - GNC algorithm performance
    - Geometric collision risk
  - On the **client** side:
    - any event that could result in an increase of the overall collision risk
- Compute the resulting probability of collision **on each phase**
- Compute the resulting probability of collision on the **mission**



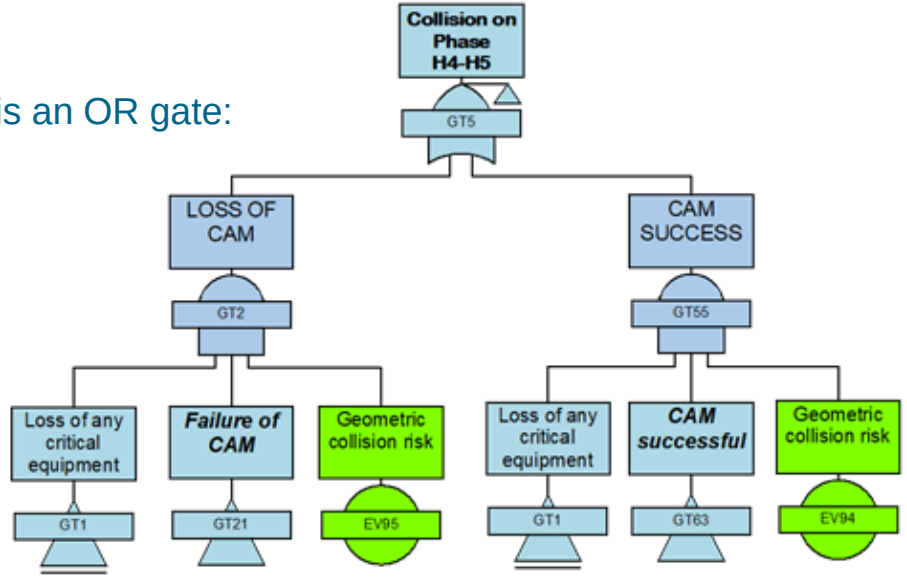
Methodology applied to the trajectory portion H4-H5 of the use case

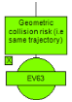
Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

COLLISION RISK ASSESSMENT

/// Fault Tree modelling – the top feared event COLLISION is an OR gate:

- The collision happens **IF** :
  - Failure of a critical equipment, requiring to perform a CAM
  - **AND** CAM fails
  - **AND** The Servicer and the Client are on the same trajectory
- **OR** :
  - Failure of a critical equipment, requiring to perform a CAM
  - **AND** CAM performed but after S/C reconfiguration (e.g. SEE)
  - **AND** The Servicer and the Client are on the same trajectory, CAM too late leading to collision



Symbol	Name	Causal relation or meaning
	**OR**	Output event occurs if any one of the input events occurs
	**AND**	Output event occurs if all input events occur
	**Transfer gate**	Indicates that this part of the fault tree is developed in a different part of the diagram or on a different page
	**Basic event**	Basic event for which failure and repair data is available
	**Geometric collision risk**	Probability derived from MC simulations

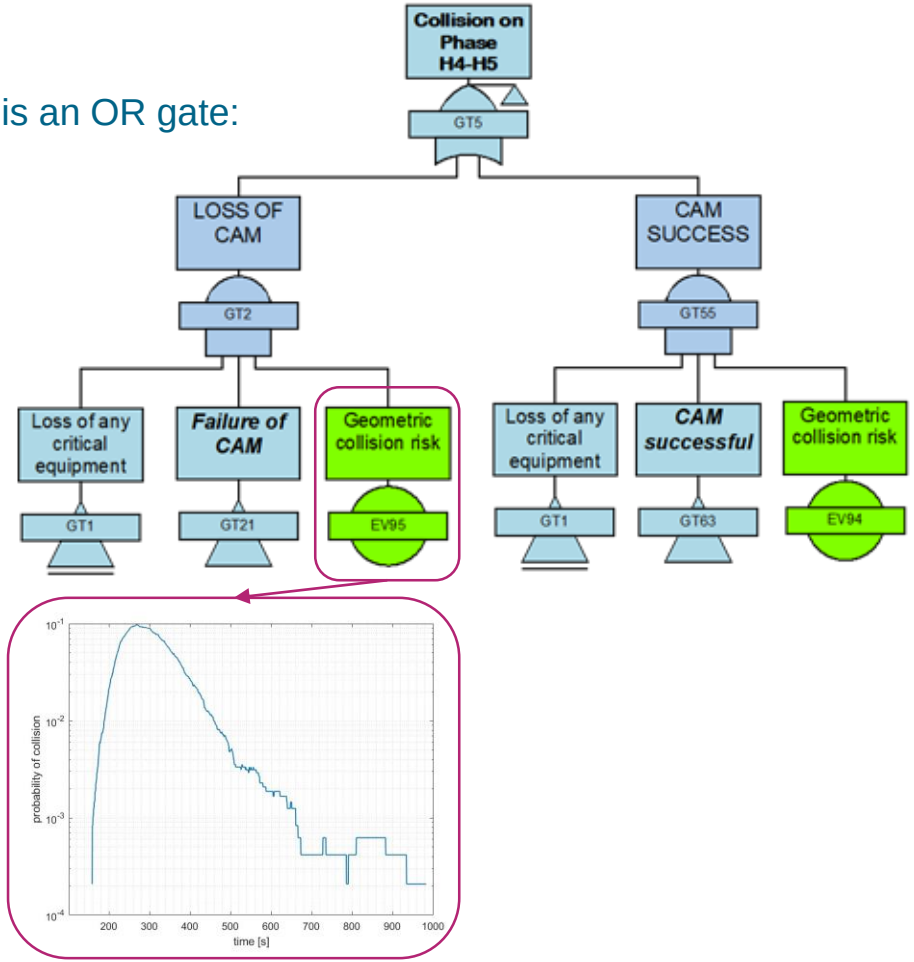
Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

COLLISION RISK ASSESSMENT

/// Fault Tree modelling – the top feared event COLLISION is an OR gate:

- The collision happens **IF** :
  - Failure of a critical equipment, requiring to perform a CAM
  - **AND** CAM fails
  - **AND** The Servicer and the Client are on the same trajectory
- **OR** :
  - Failure of a critical equipment, requiring to perform a CAM
  - **AND** CAM performed but after S/C reconfiguration (e.g. SEE)
  - **AND** The Servicer and the Client are on the same trajectory, CAM too late leading to collision

Symbol	Name	Causal relation or meaning
	**OR**	Output event occurs if any one of the input events occurs
	**AND**	Output event occurs if all input events occur
	**Transfer gate**	Indicates that this part of the fault tree is developed in a different part of the diagram or on a different page
	**Basic event**	Basic event for which failure and repair data is available
	**Geometric collision risk**	Probability derived from MC simulations



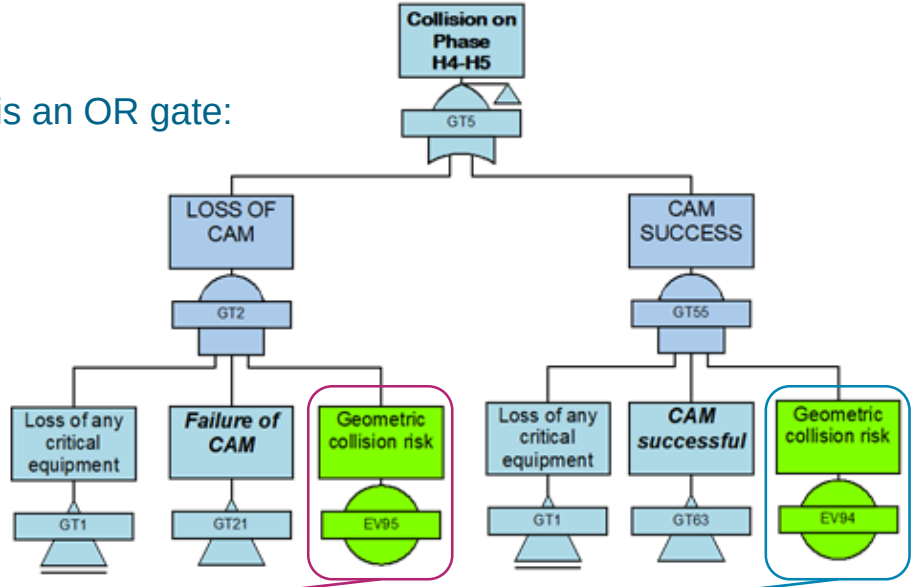
Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

COLLISION RISK ASSESSMENT

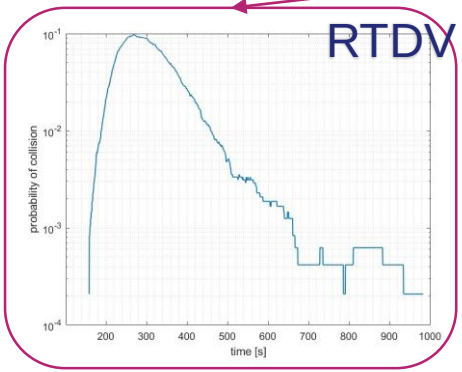
/// Fault Tree modelling – the top feared event COLLISION is an OR gate:

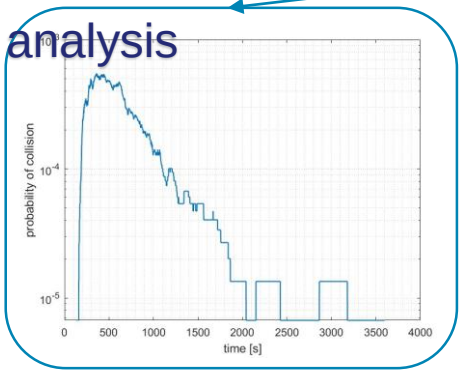
- The collision happens **IF** :
  - Failure of a critical equipment, requiring to perform a CAM
  - **AND** CAM fails
  - **AND** The Servicer and the Client are on the same trajectory
- **OR** :
  - Failure of a critical equipment, requiring to perform a CAM
  - **AND** CAM performed but after S/C reconfiguration (e.g. SEE)
  - **AND** The Servicer and the Client are on the same trajectory, CAM too late leading to collision

Symbol	Name	Causal relation or meaning
	**OR**	Output event occurs if any one of the input events occurs
	**AND**	Output event occurs if all input events occur
	**Transfer gate**	Indicates that this part of the fault tree is developed in a different part of the diagram or on a different page
	**Basic event**	Basic event for which failure and repair data is available
	**Geometric collision risk**	Probability derived from MC simulations



RTDV analysis





Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

COLLISION RISK ASSESSMENT

/// Lesson learned:

- **<u>Way forward</u> to improve this assessment:**
  - Reduce the collision risk thanks to less conservative simulations
    - Being the design of the trajectory passively safe outside the KOZ, the goal would be to focus on the final approach (forced motion)
      - Divide the forced motion trajectory in segment
      - Run MC simulation for each segment
      - Compute overall risk by taking into account the probability of having a failure in the current segment and the MC results
  - Apply this methodology on other phases of the mission
  - Apply this methodology on other phases of the mission and other type of failures (introducing change in chaser dynamic state)
- **<u>Ways to reduce the collision risk</u>**
  - At the maximum extent to have a redundancy, and ideally CAM dedicated avionic chain
  - RadHard or at least less Single Event Effect sensitive hardware
  - Hot redundancy for critical phases
  - Physical or at least functional (ex. different algorithms) redundancy of GNC
  - Slower approaches (longer duration but less risky) in order to reduce the geometric collision risk

TABLE OF CONTENTS

COMPATIBILITY ANALYSIS

/// Plume impingement:

- Three major effects can be distinguished for plume impingement:
  - Forces exerted on the client vehicle by the plume pressure
  - Heat load on the structure of the client vehicle by the hot plume gases
  - Contamination of the surface of the client vehicle by the combustion products and unburned propellant components

- To be mitigated from design:
  - Thruster accommodation and orientation
  - Final braking burn sizing
  - Release device to create an opening at departure
  - Dedicated modes for the client during capture/separation

- Analysis to support V&V
  - Systema/plume, CFD analysis, to assess (in accordance with ECSS-E-ST-35C Rev. 1)
  - Output of analysis
    - Forces/torques on the client (-> might induce tumbling on the cooperative client, whose control might be disabled during the capture phase)
    - Heat load
    - Contamination of client surfaces (& sensors)

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

COMPATIBILITY ANALYSIS

/// Electrical and Magnetic Compatibility: current and voltage interaction caused by

- ***Conduction*** (after the physical connection) **ESD (ElectroStatic Discharge)**
  - If an electrical connection between client and servicer is foreseen during the stack configuration phase, by design the first interaction should be mechanical in order to equalize any voltage difference before the realization of the electrical connection.
  - At least a simplified electro-magnetic analytical model of each satellite have to be built in order to derive the worst case electrical path of this impulsive current
  - Possibility of solutions to mitigate ESD:
    - Passive devices to equalize static charges
    - Active systems (e.g., Plume)
  - Existing tools are well established (in the sense that are widely used), however big margin are still taken (tools are not fully verified so the margins that are taken are , so worst case figures are always adopted)

- Electromagnetic field (**Electro Magnetic Compatibility, EMC**):
  - To ensure that communications between the S/Cs and ground are not affected by the proximity between the two objects
    - separation between the client and the servicer uplink/downlink carriers frequencies
    - proper choice of the relative attitudes and trajectories during the final phase of the approach
    - Analysis of shadowing effects
  - In LEO, satellites can be equipped with magneto-torquers and magnetometers, which can be affected by the emitted field of the antennas of the other satellite. Analysis should demonstrate that this effect is taken into account and that mitigation measures exist.

COMPATIBILITY ANALYSIS

/// Other types of interaction

- Thermal:
  - Shadowing effects to be taken into account
  - Refueling: avoiding any activation/explosion (dedicated analysis & test benches)
  - Thermal state of the client to be taken into account if TIR is used
  - Thermal dilation/contraction (impacting on mechanical analysis of capture sequence)
- Power:
  - power budget should include analysis on the impact of CPO & stack configuration
    - power reduction due to shadowing caused by the other satellite
    - design and operational strategy to guarantee clearance of solar arrays
  - shadowing effects of the servicer on the client might a trigger safe mode -> to be taken into account on the client side
- GNC:
  - Potential blinding of client sensors (e.g., star trackers):
    - Due to plume impingement
    - Due to active instruments such as LIDARs
  - GNSS multipath effects due to the close proximity between the two satellites

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TABLE OF CONTENTS

CAPTURE AND SEPARATION PHASES

/// Mechanical analysis and tests to V&V the capture and separation sequences:

- Capture
  - The mechanical loads sustained shall be below the thresholds such that:
    - No debris is generated
    - Continuation of nominal operations is preserved (cooperative clients only)
  - Structural dynamics analysis, multi-body analysis, static shock tests to identify envelope of sustainable loads
  - This is translated into requirements for the GNC system (e.g., control box and maximum residual rate for berthing, accurate and stable orientation and maximum misalignment for docking, etc.)
- Separation
  - Per design, the release mechanism and the separation sequence have to be designed so that the attitude and the angular rates are within the maximum acceptable values required by the client and/or by the specific mission application
  - Structural dynamics analysis, multi-body analysis do identify conditions at release and assess compatibility with GNC for control takeover
- HIL testing may be used, however:
  - Zero-g facilities add too much perturbations, so the correlation is very difficult or impossible.
  - Parabolic flight are very expensive and offer limited simulation time
  - air bearing facilities are in 2DoF only (correlation can’t be done on the whole model, but only on a derived model)
  - Neutral Buoyancy Facilities are high cost facilities, even though they allow a three dimensional representation of the systems; however the inertia of the water is not compensated and the capture/separation systems must be water-proofed.

Date: 10/10/2024
Ref: -
Template: 83230347-DOC-TAS-EN-011

TABLE OF CONTENTS

CONCLUSIONS

/// Lesson learned:

- Trajectory design and validation
  - The need of a RTDV-like tool has been identified, to allow early design and validation of trajectory (nominal and contingency) with the need few(er) hypothesis (wrt to a FES), and faster simulation time
  - LCA is a powerful tool for preliminary trajectory design, but MC analysis are needed for the validation phase
  - Importance of considering orbital perturbations since the preliminary trajectory CONOPS definition, especially if the client and the servicer have a considerable difference in the coefficients (SRP in GEO, ballistic in LEO)
  - Though not required by requirements, the use of passively safe trajectories is advisable since it simplifies the safety approach
- Collision risk assessment
  - The need of standardization & validation of a methodology has been identified.
  - Hybrid approach RAMS & GNC (FTA + RTDV tool/FES at later stages)
  - Thales Alenia Space methodology is still under refinement and will be applied for the EROSS-SC programme overall collision risk assessment
- Compatibility analysis
  - No need to develop dedicated tools identified
  - CPO specific analysis need to be performed and compatibility of the E2E service with the client should be ensured by design
  - Information sharing between the client entity and the servicer entity is fundamental
- Capture and Separation phases
  - Strong coupling between mechanical aspects and GNC
  - Fully representative HIL testing not possible

END OF THE PRESENTATION

ACKNOWLEDGEMENTS:

The Authors want to acknowledge the **European Space Agency ESA** and the industrial partners **DEIMOS** and **GMV** for their fruitful support and collaboration on the study "*Verification and Validation of Rendezvous and Proximity Operations Safety*", which was financed under an ESA contract issued with the invitation to tender AO11351